Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 3 | Mar 2017

SECURE MULTI-OWNER TRANSACTION USING VISUAL CRYPTOGRAPHY

Prof. P. S. Nawghare [1] | Priyanka Gogawale [2] | Aishwarya Bhosale [3] | Sampada Thorat [4] | Payal Gambre [5]

[1] Assistant Professor, Department of Computer Engineering, Zeal College of Engineering and Research Narhe , Savitribai Phule Pune University, India.

[2] Student, Department of Computer Engineering, Zeal College of Engineering and Research Narhe , Savitribai Phule Pune University, India.

ABSTRACT

Secure Multi Owner Transaction System Using Visual Cryptography (VC) aims at providing a facility to make secure banking transaction for corporate world. It has the flexibility to allow request of transaction from any remote place, even when key stakeholders of transaction process are not available at workplace. This is enabled by implementing the VC in Secure Multi Owner Transaction System. The transaction is proceed in full confidentiality by applying appropriate security measures to allow the owners to agree for any participating owner only if he logs into the system by entering the correct password which is generated by merging the two shares (Black & White dotted Images)using VC scheme. Owners will get the secret password to perform his transaction successfully by combining all shares according to the number of owners using VC .Visual Cryptography (VC) is a secret sharing scheme in which an image is converted into shares. No information can be revealed by observing any share (Black & White dotted Image). The information about the original image (Voter Password) will be revealed only after stacking sufficient number of shares. There are various schemes present in VC, 2 out of 2, k out of n, n out of n, etc. In the proposed method, IVS with n-out-of-n VC has been used for an efficient authentication system. Even if the hacker gets one share of the password, it is impossible to get the other share of the password, as it will be sent to the E-Mail Id of the owner. Thus Our system provides two way securities to the banking transaction, which is very much in need.

KEYWORDS: Multi-Owner Transaction ,Secure Share Scheme, Visual Cryptography

I. INTRODUCTION

Online money transfer is an essential exercise for most of the people now a days. Internet banking has eased our life by providing the facility of online money transfer. Within every transaction, we get a message alert to our registered mobile. This is High Security One Time Password (OTP) and is very important for the security of our account. Every time you write the password in the box and approve. The bank shall take reasonable care to, ensure security of and prevent unauthorized access to the internet banking services using technology available to the bank. The internet is susceptible to various cyber crime like fishing, vishing (voice fishing), SMSing (fishing through SMS),compromise of user system security etc., that could affect Payment Instruction/other instruction to the bank. Bank does not held any responsibility for the losses arising out of such cyber crime. User have to separately evaluate all such risk. Thus there is need of security for secure transaction.

1. TRADITIONAL SYSTEM

In single mode operation only one account holder is operating his\her account. He is aware about all the transactions which are carried out in his account. So there is no issue of fraud transactions.

Joint accounts: There are different types of joint accounts offered by bank, based on the mode of operation & accessibility as follows:

Either or Survivor: This is a most common form of joint account. Only two individuals can operate the account i.e, primary account holder & secondary account holder both access the account & transfer the funds.

Anyone or Survivor: This is similar to "either or survivor" .The only difference is more than two individuals can operate the account.

Former or survivor: In this type of joint account only the first(primary) holder can access &operate the account till the time of she or he is alive. The second holder can operate the account only on the death of primary holder.

In case of Joint Accounts, transactions through Internet Banking, shall be available if the mode of operation is indicated as 'either or survivor' or 'anyone or survivor'. If You are desirous of using the Internet Banking, You should either be the account holder and sole signatory or authorized to act independently in case of a joint account. For such joint accounts, one User-Id and password for Internet Banking will be issued to each of the joint account holders when requested. The other joint account holders shall expressly agree with the arrangement and give their consent on the application form for use of Internet Banking. In case of joint accounts operated by more than one person, Bank shall act on the instruction received first and any subsequent instruction shall be neglected. All correspondence will be addressed to the first named person only. All transactions arising from the use of Internet Banking in the joint account shall be binding on all the joint account holders, jointly and severally.

1.1 DISADVANTAGES OF TRADITIONAL SYSTEM

No Internet Banking service is available for "Former and Survivor" mode of operation in Joint account. Only primary account holder is allowed for Internet Banking. The permission for transaction is taken from all account holder in only written form. It is time consuming process. There issues are arises due to misuse and abuse of joint account by primary account holder.

2. MULTI-OWNER SYSTEM

To overcome issues arises in to traditional system we propose multi-owner system. IN this system ,if primary account holder is request for transaction, server will proceed only if all other account holder agreed for it the transaction. The permission is taken from all account holder via mail. Thus misuse and abuse of joint account by primary account holder should be reduces.

3. VISUAL CRYPTOGRAPHY

VC is used to encrypt written material (printed text, handwritten notes, pictures, etc). The decoding is done by the human visual system directly (By stacking share one over the other). For a set P of n participants, a secret image S(owner password) is encoded into n shadow images called shares, where each participant in P receives one share . To retrieve the image back all the participants share has to be place one over another then the image is got. Using VC in Secure Multi-Owner Transaction System aims to make reliable banking transaction .Because transaction can be carried out only when all the owners are agreed for the transaction. Thus system overcome the issues in fraud transaction.

There are many visual cryptography schemes in existence. A selection are described below 1.1. 2 out of 2 Visual Cryptography Scheme In this type of visual cryptography scheme, the secret image is divided into two shares. This is the simplest kind of visual cryptography. The major application of this scheme is found with IVS that uses 2 out of 2 Visual secret sharing schemes for authentication purpose. To reveal the original image, these two shares are required to be stacked together.

3.1 N OUT OF K VISUAL CRYPTOGRAPHY

This kind of scheme allows dividing a secret image (secret data) into k number of shares. Then the secret image can be revealed from any n number of shares among k. For example, In 3 out of 6 VC scheme, any 3 shares out of 6 shares are sufficient to reveal the secret data. The major problem associated with this scheme is that the user needs to maintain many shares which may result into loss of shares. Also more number of shares means more memory consumption.

3.2 K OUT OF K VISUAL CRYPTOGRAPHY

Here original secret is divided into k number of shares and for reconstruction of the secret, all k shares are necessary. For example, in 6 out of 6 VC scheme, Secret is revealed only after stacking all the 6 shares, where k= 6. This scheme

is not so popular because managing k number of shares is difficult task and it also increases time complexity.

II. LITERATURE SURVEY

Ankasha Bandil and K.V.Arya[1] propose a multiple image sharing scheme for secure communication of multiple images. For this scheme (k, n) secret scheme is used. The proposed scheme is applied for digital information data to provide a secure transmission, in such a way that only receiver get appropriate information. The proposed scheme, secretly generates n number of shares for multiple images by applying the matrix multiplication and matrix addition method with the help of random matrix under the deformation algorithm in such a way that single share does not reveal any information about the secret images. Receiver only get shares of secret image send a subset of shares is used to identify the secret images. Experimental results shows that the proposed scheme is efficient, simple and secure for transferring images in wireless mode. For this scheme (k, n) secret scheme is used. Fang and Lin's [2]scheme combine the principle of traditional visual cryptography with authentication characteristic, when we fix the first share image and shift the other share image for certain unit, we can obtain the extra confidential data. But in traditional visual cryptography, secret pixels are expanded to cause the size of the recovered image is larger than the original one. So this study combined the non-expanded scheme with the extra ability of hiding confidential data to prevent the detection of information. They use block encoding technique with non expansion ability. Maruti Deshmukh and Nita Nain[3] propose scheme of An (n, n)-Multi Secret Image Sharing Scheme using Boolean XOR and Modular Arithmetic Secret sharing scheme is an efficient method of transmitting one or more secret images securely. The traditional visual secret sharing schemes share only one secret image at a time. With the advancement of time, there arises a need for sharing more than one secret image. An (n, n)-Multi Secret Image Sharing (MSIS) scheme is used to encrypt n secret images into n meaningless shared images and stored it in different database servers. For recovery of secrets n shared images are required. If loss of any shared image then no secret images are recovered.

III. PROPOSED SYSTEM

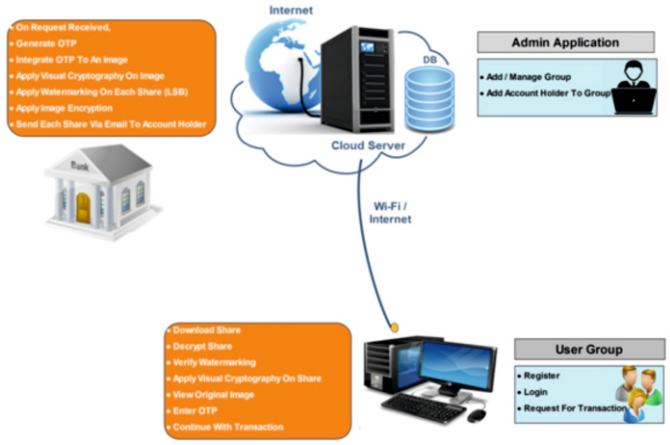

FIG 1: PROPOSED SYSTEM

There are mainly four component of system that are users, admin, transaction panel and cloud server. In system architecture there is one admin application. First admin must be login in to system. Admin application adds and manages the group of user. Admin will also add account holders to group. Second there is one user application. user must be register with their email id and password. User should login in to system with their email id and password .Then user also check the group of user which user is belong. Then user will request for the transaction. On the cloud server firstly request is received. Then system will generate OTP that is one time password. After that OTP is convert in to the image. Then visual cryptography is applied on OTP image. Water marking technique also applied. That image is divided in to according to number of user. Each share of image is encrypted and send each share of image via email to each account holder. Then again on transaction panel each user will download share which is send by email id. Then each share of image will decrypted. Also verify the watermarking technique and apply visual cryptography. Then integrate shares of images in to single image. If the original image and generated image is same then continue with transaction. If generated image does not match with original image then transaction is fail.

IV. ALGORITHM

The proposed scheme is suitable for grayscale and colored images. In proposed scheme, n secret images Ii, $i = 1, 2, \bullet\ \bullet\ \bullet, n$, are encoded into n shared images Si, $i = 1, 2, \bullet\ \bullet\ \bullet, n$. First the temporary shares Ti, $i = 1, 2, \bullet\ \bullet\ \bullet, n$ are generated using additive modulo operation on secret images Ii, $i = 1, 2, \bullet\ \bullet\ \bullet, n$. Finally, shared images Si, $i = 1, 2, \bullet\ \bullet\ \bullet, n$ are generated using reverse bit operation on temporary shares. The sharing algorithm of proposed (n, n)-MSIS scheme is given in Algorithm 1.

Algorithm 1: Sharing Procedure.

Input: n secret images $\{I1, I2 \bullet\ \bullet\ \bullet\ In\}$.

Output: n shared images $\{S1, S2 \bullet\ \bullet\ \bullet\ Sn\}$.

1. Generate temporary shares using additive modulo

$T1 = (I1) mod 256$

$Ti = (Ii + Ti-1) mod 256$, where $\{i = 2, 3, \bullet\ \bullet\ \bullet, n\}$

2. Create shared images using reverse bit

$Si = ReverseBits(Ti)$, where $\{i = 1, 2, \bullet\ \bullet\ \bullet, n\}$

The recovery procedure is just reverse of the encryption algorithm. The time required to share n secret images is same as that of the time required to recover n secret images. The temporary shares are obtained using reverse bit operation on shared images. Recovered images are obtained after performing additive inverse operation on temporary shares, Ti, $i = 1, 2, \bullet\ \bullet\ \bullet, n$ which is same as that of the secret images. The recovery procedure of proposed (n, n)-MSIS scheme is given in Algorithm 2.

Algorithm 2: Recovery Procedure:

Input: n shared images $\{S1, S2 \bullet\ \bullet\ \bullet\ Sn\}$.

Output: n recovered images $\{R1, R2 \bullet\ \bullet\ \bullet\ Rn\}$.

1. Recover temporary images using reverse bit

$Ti = Reverse\ Bits(Si)$, where $\{i = 1, 2, \bullet\ \bullet\ \bullet, n\}$

2. Recovered secret images using additive inverse

$R1 = (T1) mod 256$

$Ri = (Ti - Ti-1) mod 256$, where $\{i = 2, 3, \bullet\ \bullet\ \bullet, n\}$

V. CONCLUSION

This system is designed for corporate companies to make their multi-owner transactions securely. Even though the all of the owners are situated in different paths of the country or the world, the transaction can be conducted easily & effectively in a proper manner by using Secure Multi-Owner Transaction System Using Visual Cryptography. Our system offers many benefits including trustworthy internet banking & increase security in transaction. It provides owners with reliable and intuitive indications of validity of the transaction process system. The proposed system uses visual cryptography to provide mutual authentication for owners and transaction servers.

VI. REFERENCES

[1] Blundo, Carlo, et al. Multi-secret sharing schemes. Advances in Cryptology CRYPTO94. Springer Berlin Heidelberg,(1994.)

[2] Yang, Ching-Nung, Cheng-Hua Chen, and Song-Ruei Cai. Enhanced Boolean-based multi secret image sharing scheme. Journal of Systems and Software (2015)

[3] Lin, Tsung-Lieh, et al. A novel visual secret sharing scheme for multiple secrets without pixel expansion. Expert systems with applications 37.12 (2010)